

CHIFFRES EN FOLIE: LE COÛT DES CYBERATTAQUES

LE 11 JUILLET 2011 ALEXANDRE DELAIGUE (ECONOCLASTE)

D'après les éditeurs de solutions de sécurité, les attaques informatiques coûteraient 1000 milliards de dollars aux États par an. Problème: personne ne peut le prouver. Alexandre Delaigue désosse ces représentations.

On a récemment attiré mon attention sur **cet article du Figaro, dont l'auteur essaie d'évaluer le coût des cyberattaques**. Le désarroi de l'auteur de l'article est visible : ayant cherché diverses sources d'information, il a bien du mal à relever la moindre cohérence. Un chiffre, surtout, sort du lot : selon une étude commandée par McAfee, en 2008, les cyberattaques auraient coûté environ 1.000 milliards de dollars à l'économie mondiale, soit 1.64% du PIB mondial (admirez la précision des deux chiffres après la virgule).

Un chiffre comme celui-ci, aussi rond qu'énorme (aujourd'hui, c'est à partir de plusieurs centaines de milliards de dollars qu'un problème devient important : ça n'arrange pas les affaires du **Dr Evil**) suscite les soupçons. Il est totalement incohérent avec les autres évaluations données dans l'article : si les cyberattaques coûtent 560 millions de dollars en 2009 aux USA, comment atteindre les 1000 milliards de dollars dans le monde en 2008?

J'avais montré, il y a quelques temps, que le **coût mondial de la contrefaçon était estimé d'une manière absurde**, avec un chiffre totalement faux qui subsistait obstinément dans toutes les évaluations, avec untel qui cite le chiffre en faisant référence à machin, lequel le tient de bidule, qui le tient lui-même d'untel. Ce chiffre de 1.000 milliards de dollars pour le coût des cyberattaques est en train de suivre le même processus. L'article indique ainsi que le chiffre a été cité lors d'un **forum des Nations Unies sur la cybersécurité** [pdf], qui fait référence à des données d'Europol, qui elle-même fait référence... à l'étude de McAfee. C'est comme cela qu'un chiffre finit par "faire autorité", pour reprendre les mots de l'auteur. Mais comment ce chiffre a-t-il été déterminé ?



Montant totalement inventé

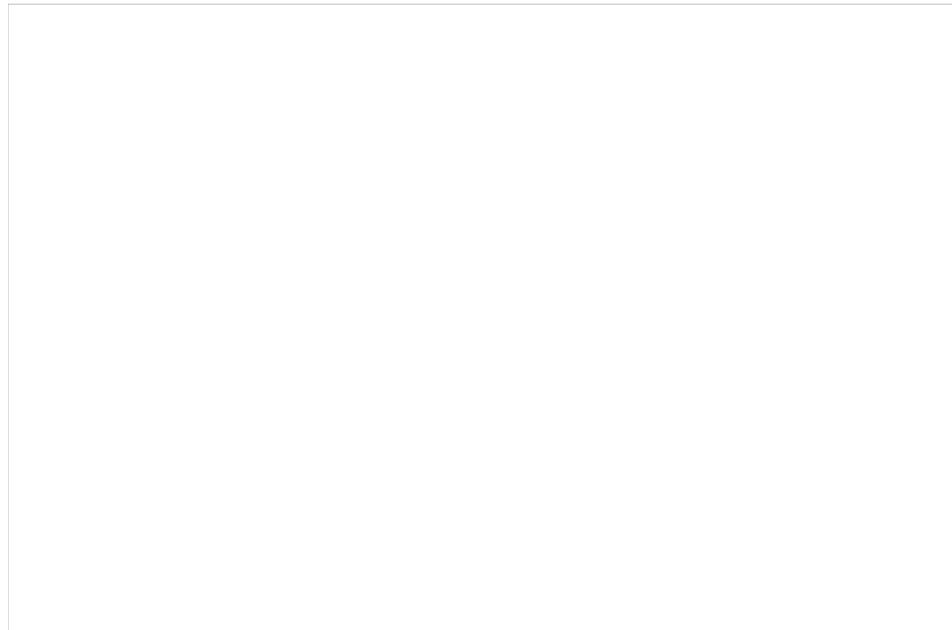
Je suis donc allé voir cette fameuse étude commanditée par McAfee en 2008, sur le coût du cybercrime. Vous pouvez aller **consulter le rapport ici** [en, pdf]. Et surprise : le chiffre de 1.000 milliards de dollars n'y figure nulle part. Ce chiffre a été en fait cité pour la première fois **par le président de McAfee, au forum de Davos** [en]. Il déclare que le rapport "montre que le coût du cybercrime est de 1.000 milliards de dollars par an, ou plus". Alors que jamais le

rapport n'évoque ce chiffre !

Le premier surpris par ce chiffre est d'ailleurs... **un contributeur du rapport** [en] qui se demande d'où il peut venir. Une façon d'expliquer comment ce chiffre peut être tiré du rapport **est la suivante** [en] : ce rapport a été établi à partir d'entretiens auprès de 1.000 cadres dirigeants d'entreprises (environ 500 entreprises interrogées), qui estiment en moyenne avoir perdu 4.6 millions de dollars de propriété intellectuelle en moyenne au cours de l'année 2008. On peut alors peut-être supposer que les 1.000 milliards sont établis en considérant que cet échantillon est représentatif (ce qui est parfaitement absurde) et en l'appliquant à l'économie mondiale. Mais impossible d'en être certain : jamais la moindre méthodologie n'est indiquée, nulle part. Ce chiffre est donc totalement inventé, et légitimé en citant un rapport qui n'y fait jamais allusion.

Et ça ne l'empêche pas d'être cité comme *"faisant autorité"*, repris par toutes sortes d'organismes. Certains même, voulant sans doute avoir l'air sérieux, affirment que *"le vrai chiffre doit être plus élevé"* parce que l'évaluation date de 2008... On attend impatientement les calculs qui montreront triomphalement qu'étant donné que le cybercrime "coûtait 1.000 milliards de dollars en 2008" et que la croissance économique a depuis été de tant, il faut réévaluer ce chiffre à 2.000 milliards... Ne riez pas, ça sera certainement fait.

On pourrait se demander pourquoi un chiffre aussi bidon se retrouve cité et repris partout, au point de *"faire autorité"*. Le facteur principal est bien connu : citer des nombres est en soi un argument d'autorité. La phrase *"la criminalité a augmenté depuis l'année dernière"* a beaucoup moins de poids que *"la criminalité a augmenté de 4.5% depuis l'année dernière"*. Je viens d'inventer ce chiffre : pourtant, convendez que la seconde phrase a l'air beaucoup plus crédible. Elle donne l'impression que je sais de quoi je parle, qu'une mesure a été effectuée, alors que mon chiffre n'a strictement aucune signification.



Le grand problème global

On pourrait certainement faire le même genre de décryptage avec la déclaration de L. Wauquiez, selon lequel **"un internaute sur 30 a perdu de l'argent à cause d'un pirate informatique en Europe au cours des 12 derniers mois"**. Comme toujours dans ces cas-là, le chiffre est repris et cité, sans la moindre façon de savoir d'où il est sorti (l'article cite encore d'autres chiffres sur le revenu issu des cyberattaques, bien évidemment, toujours aussi invérifiables). On constate aussi que la *"guerre au cybercrime"* consiste surtout à **mélanger des choses qui n'ont rien à voir les unes avec les autres**, pour faire de questions différentes un grand problème global exigeant des solutions (et des ressources) importantes.

Le but n'est pas de dire que les cyberattaques n'ont aucune importance, ni aucun coût, qu'il ne faut pas y prêter attention. Simplement de rappeler que les coûts, en la matière, sont très difficiles à évaluer. Et que ceux qui multiplient les chiffres sans signification le font soit comme argument commercial (comme le fait McAfee) soit pour légitimer leur action et mettre en œuvre le **théâtre sécuritaire** [en] (comme les politiques ou administrations qui multiplient la citation de ce genre de chiffres pour montrer que le gouvernement travaille).

Hystérie collective

Il s'agit simplement de rappeler que l'exagération des menaces, à l'aide de chiffres sans signification, finit par avoir des conséquences lourdes. Si je me fais voler 100 euros, le vrai coût social de ce vol n'est pas 100 euros qui ont simplement été transférés d'une personne à une autre : il vient parce que je vais changer de comportement, consacrer plus de ressources à ma protection au lieu de les consacrer à des usages plus utiles. Si un pirate informatique obtient mon numéro de carte bancaire, c'est énervant, mais pas dramatique (il suffit de changer la carte prématurément). Si un hacker révèle les caractéristiques du prochain iPad et sa date de sortie, conduisant de nombreux acheteurs potentiels à attendre ce nouveau modèle plutôt que d'acheter l'existant, cela représente évidemment un préjudice pour Apple, mais plutôt un avantage pour les consommateurs. Si des hackers avaient vraiment réussi à obtenir les **documents de Bercy consacrés au G20**, ils auraient surtout constaté et révélé la vacuité de la chose. Pour les États-Unis, le coût du 11 septembre n'est pas tant le coût direct (morts, destructions) que l'ensemble des mesures qui ont été prises en réaction (deux guerres, sécurité des aéroports, morts sur les routes de gens qui ont renoncé à prendre l'avion, etc).

Le coût principal de la criminalité tend à survenir lorsqu'on décide d'y accorder trop d'importance, en négligeant la résilience sociale, et en y consacrant des ressources qui auraient été bien plus utiles ailleurs. Multiplier les évaluations fantaisistes et alarmistes du coût des cyberattaques remplace la question raisonnable : "*quelles ressources, qui pourraient être utilisées à autre chose, faut-il consacrer à ce problème ?*" par une hystérie collective dans laquelle jamais rien ne sera suffisant pour calmer les inquiétudes, parce que la sécurité absolue ne saurait être atteinte. Cette hystérie en enrichit quelques-uns, au détriment de l'ensemble.

Article initialement publié sur Econoclaste

Crédits photo: Flickr CC [kmichiels](#), [Curtis Gregory Perry](#), [bartb_pt](#)

NICOLAS

le 11 juillet 2011 - 9:17 • SIGNALER UN ABUS - PERMALINK



Merci de votre article qui remet les points sur les i. La source originale des 1000 milliards de dollars faisant de la cybercriminalité un trafic plus rentable que le trafic de drogue (accroche originale des articles de l'époque citant pour la première fois ce chiffre) est une audition devant le Sénat américain d'un responsable de AT&T <http://www.net-security.org/secworld.php?id=7239>

Ensuite concernant le journaliste du Figaro.fr, il m'avait interrogé et je lui ai fourni toutes ces études (dont la source ci dessus) en lui expliquant que ces chiffres étaient peu pertinents et très contestables. Il voulait absolument des chiffres surtout français. Mais en effet comme cet article le souligne aucune étude sérieuse n'existe. Les chiffres sont inventés. Et repris comme le référentiel mondial.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

PINTEJEAN-PAUL

le 11 juillet 2011 - 10:17 • SIGNALER UN ABUS - PERMALINK



Tout à fait OK Comme Nicolas ci-dessous, il s'agissait de savoir s'il existait des études et des chiffres pertinents sur le sujet et je lui ai fourni également l'ensemble de mes données et sources.

J'ai aussi insisté sur le fait qu'il était difficile d'accorder une crédibilité à ces chiffres aujourd'hui...

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

NICOLAS

le 11 juillet 2011 - 17:56 • SIGNALER UN ABUS - PERMALINK



Par contre, il ne m'a pas cité comme source... Sympathique comme on peut mâcher le travail de certains journalistes qui, en plus, n'analysent pas jusqu'au bout les données qu'on leur fournit.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

ALEXANDRE DELAIGUE

le 11 juillet 2011 - 18:35 • SIGNALER UN ABUS - PERMALINK



@ Nicolas et Jean-Paul Pinte,

Merci de vos retours. L'intérêt des éléments que vous avez fourni à l'auteur de l'article était précisément de montrer la faible fiabilité de ces chiffres. Concernant le meme des 1000 milliards, après recherche, le responsable d'ATT faisait référence au FBI, qui lui même se réfèrait... Au président de McAfee. C'est regrettable parce que cette énorme imprécision ne facilite pas une prise en compte raisonnable du problème.

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

NICOLAS

le 11 juillet 2011 - 18:42 • SIGNALER UN ABUS - PERMALINK



Pour continuer le débat : un lien intéressant pour parler de sécurité informatique et économie et chiffres <http://weis2011.econinfosec.org/program.html>.

Une présentation tout à fait dans le sujet : <http://weis2011.econinfosec.org/papers/Sex,%20Lies%20and%20Cyber-crime%20Surveys.pdf>

Comment inventer des chiffres bidons.

Bonnes lectures !

Nicolas Caproni

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE